Qualys WAS Lab Tutorial Supplement

TABLE OF CONTENTS

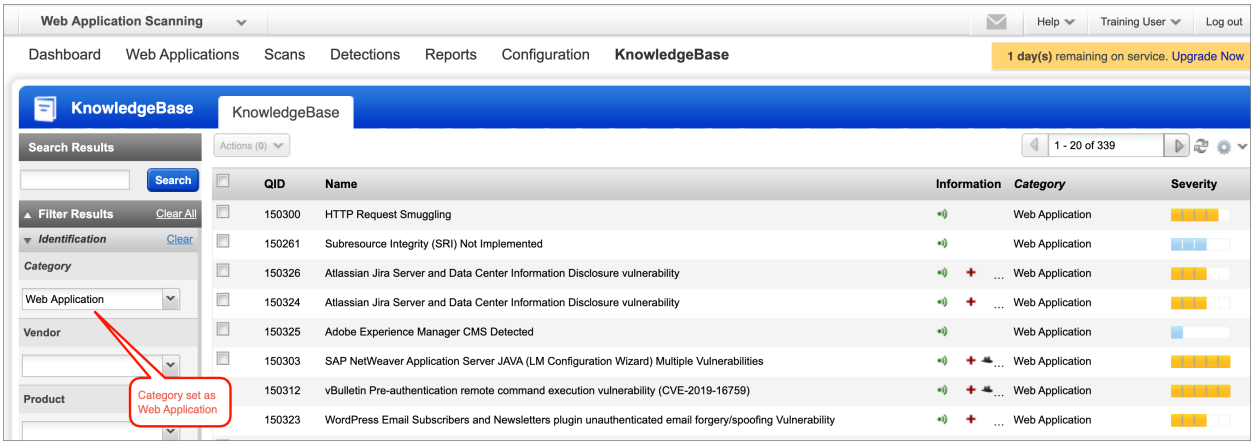
Qualys Web Application Scanning (WAS) enables organizations to assess, track, and remediate Web application vulnerabilities. With BURP integration, manual Web application testing results can be combined with the automated findings produced by WAS. The Qualys Malware Detection (MD), is a standard component in WAS, providing malware monitoring on top of vulnerability detection.

The Open Web Application Security Project (OWASP) Top 10 list has become the industry standard for categorizing the most critical risks faced by Web apps. Qualys WAS allows you to accurately find these vulnerabilities – including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and URL redirection – and learn how to mitigate them.

WAS KnowledgeBase

PLAY http://ior.ad/7fLC

All detectable vulnerabilities can be viewed from the Qualys KnowledgeBase. The Search and Filtering pane (left) will allow you to locate Web application vulnerabilities.



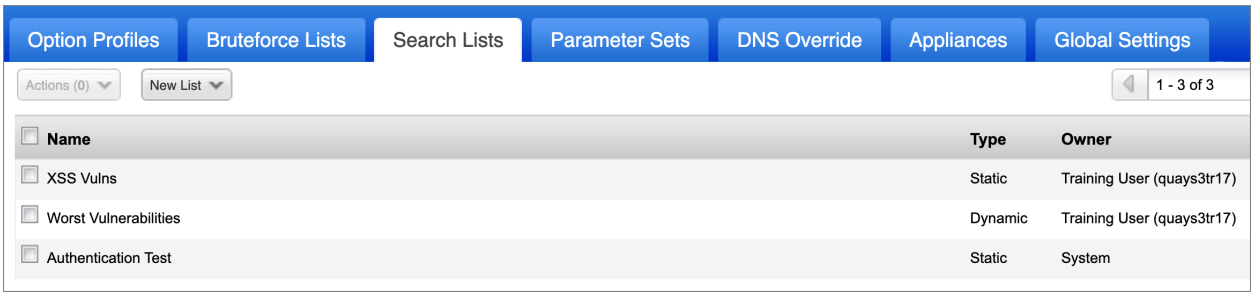
WAS Search Lists

PLAY http://ior.ad/7fmc

A “Search List” is an extension of the Qualys KnowledgeBase and is a powerful customization tool within Qualys Web Application Scanning. The name “Search List” is derived from the KnowledgeBase “Search” tool that is used to create a list of vulnerabilities. A Search List is a grouping of QIDs that can be used in various capacities in Qualys Web Application Scanning.

You can add a Search List to an Option Profile to customize your scan. For instance, you can run a scan for just a specific vulnerability. Or, you can use a Search List to omit vulnerabilities from a scan.

You can also add a Search List to a Report Template to help prioritize which vulnerabilities will be addressed first. For example, you can build a report containing only XSS vulnerabilities or only your most severe vulnerabilities.



WAS Workflow

The workflow for analyzing a Web application involves five simple steps: 1) Define Web Application, 2) Perform Discovery Scan—Crawl, 3) Perform Vulnerability Scan, 4) Create Reports, and 5) Fix Vulnerabilities

Here is a detailed view of this workflow:

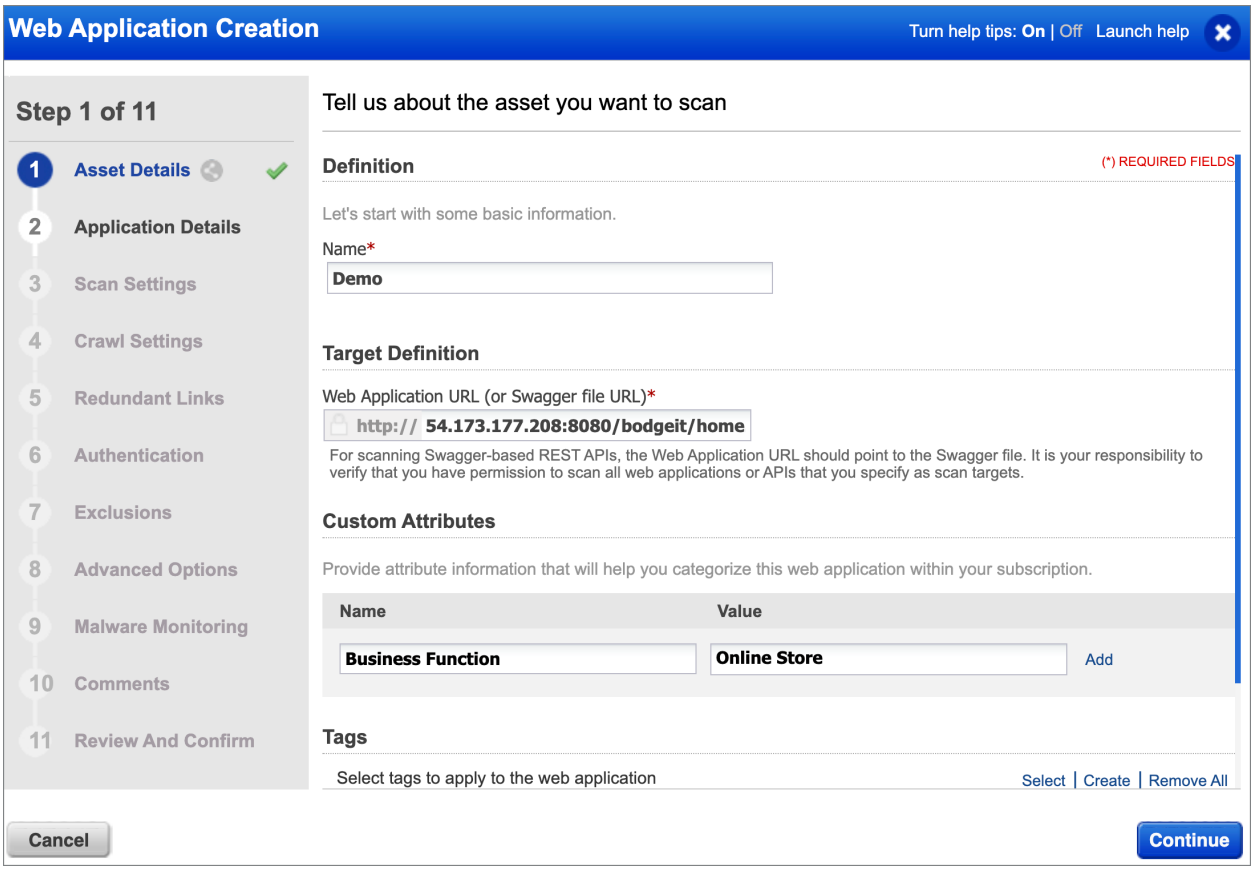
1. Define Web Application
    - Identify the location (URL) of the Web App
    - Define the “scope” of the Web App Crawl
    - Choose from various scanning options—Option Profile:
    - Select a scanner appliance
    - Include “crawling hints” and/or header injection
    - Use optional DNS Override
    - Provide authentication credentials
        - Form records
        - Server records
    - Identify areas to “white list” or “black list”
    - Enable malware monitoring
2. Perform Discovery Scan (Crawl)
3. Perform Vulnerability Scan
4. Create reports to identify links crawled and vulnerabilities detected
5. Fix vulnerabilities

Basic Application Setup

PLAY http://ior.ad/7eMQ

PLAY http://ior.ad/7eVu

Before a Web Application can be scanned, it must first be added to your WAS subscription.

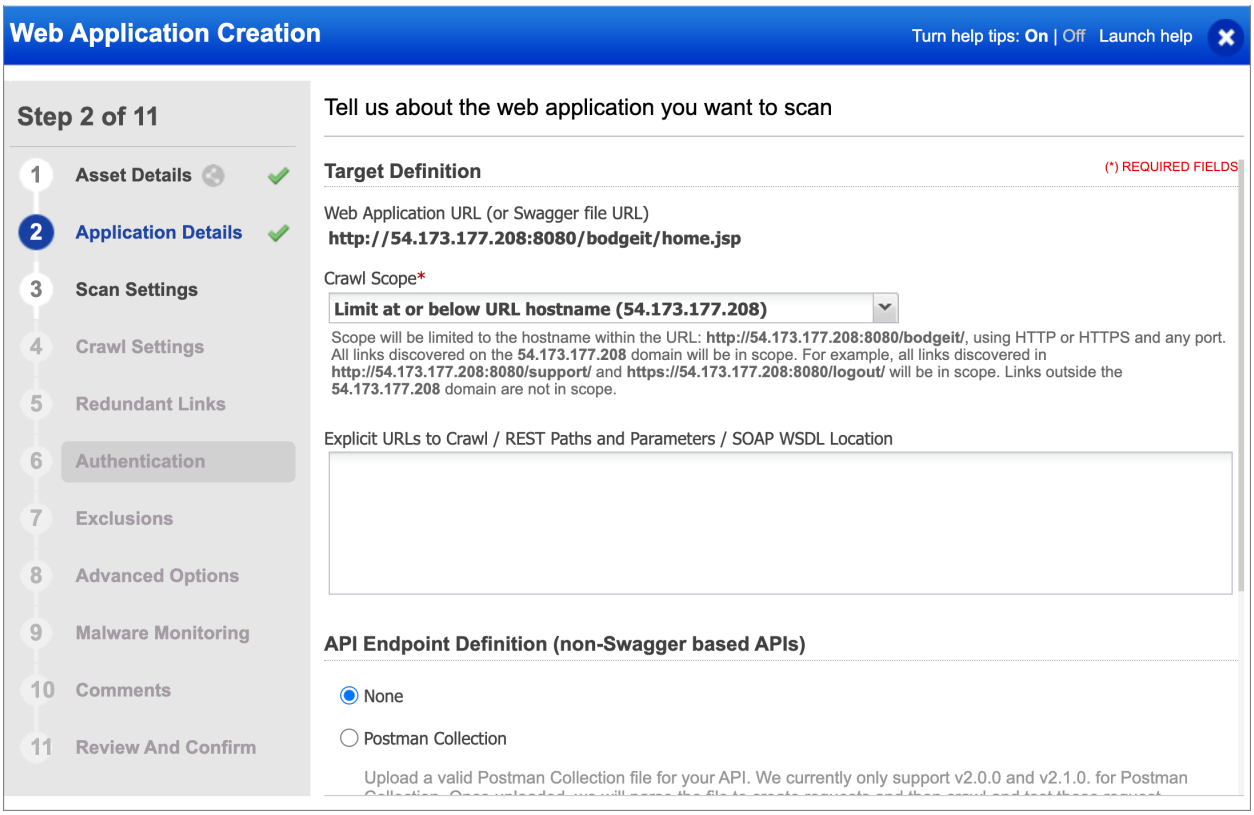


On Step 1 (Asset Details) of defining the web application, the following can be defined:

Target definition – URL of the application or the Swagger file if you're scanning API endpoints

Custom Attributes – Name/Value pairs that can be used for categorizing and filtering the application

Tags – Labels that can be applied to applications for filtering, scanning, and reporting purposes



On Step 2 (Application Details) of defining the web application, the following can be defined:

Crawl Scope – a single web application can span multiple domains, IP addresses, and port numbers (including sub-domains and subdirectories). The scope of an application defines its boundaries.

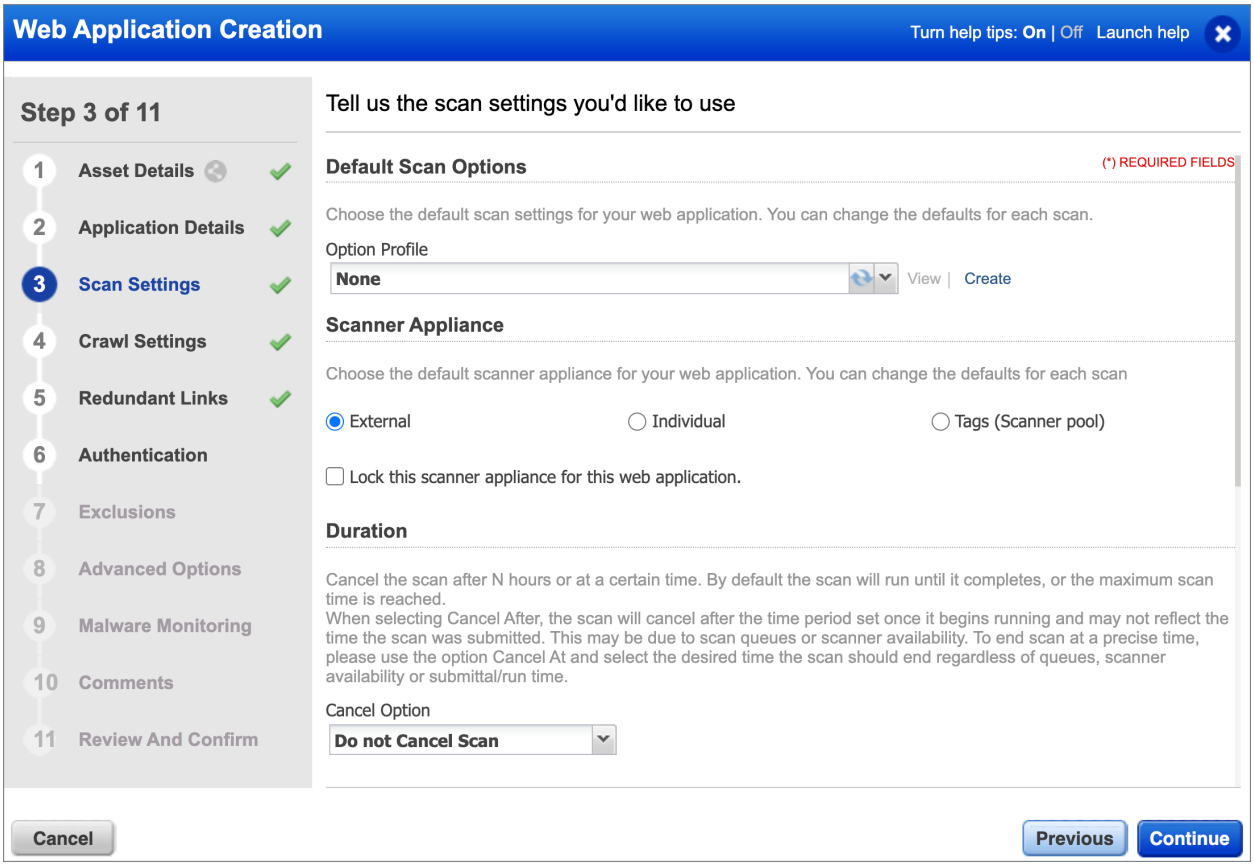
The "Crawl Scope" field provides a few options:

- **Limit at or below URL hostname** - Select to limit crawling to the hostname within the URL, using HTTP or HTTPS and any port.
- **Limit to content located at or below URL subdirectory** - Select to crawl all links starting with a URL subdirectory using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified sub-domain** - Select this option to crawl only the URL hostname and one specified sub-domain, using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified domains** - Select this option to crawl only the URL hostname and specified domains, using http or https and any port.

Explicit URLs to Crawl - this is useful for pages not directly linked to other pages within the application. For example, a registration link sent to the user via email. You can also include WSDL URLs for web services you want the service to crawl. Enter each URL on a separate line.

Each entry must be a valid http or https URL. You can enter a maximum of 2048 characters for each URL. The URLs you enter must be consistent with the selected scope.

API Endpoint Definition – for non-Swagger based APIs, you may upload a valid Postman collection or a Burp Log file with your scan tests



On Step 3 (Scan Settings) of defining the web application, the following can be defined:

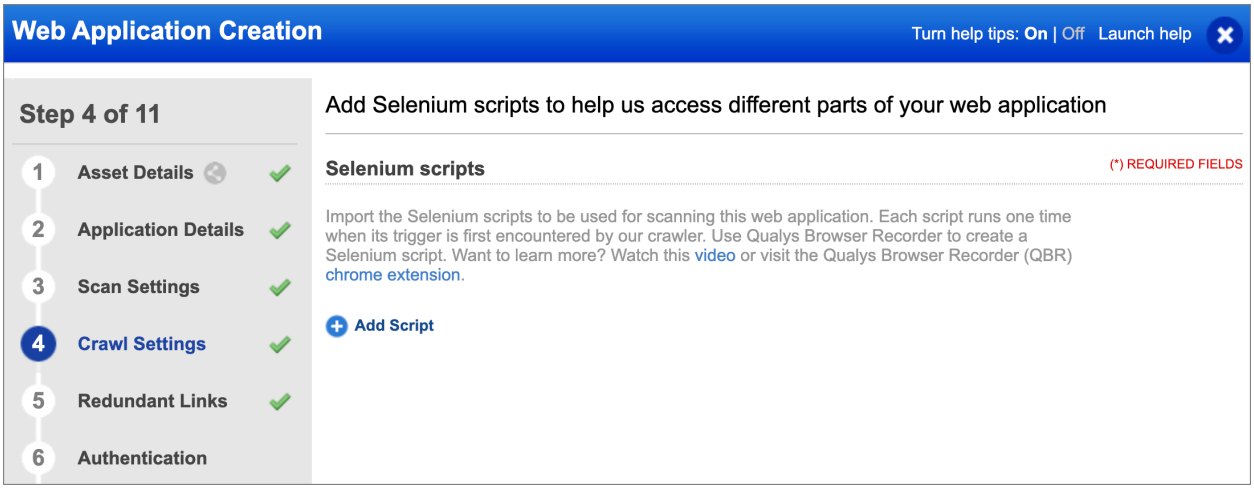
Option Profile – A collection of scan settings to be used while crawling or scanning the application

Scanner Appliance – The appliance to be used for crawling or scanning the application. Be sure the Scanner Appliance you are using has access to the application you are scanning.

Duration – How long should the scan run before being automatically cancelled

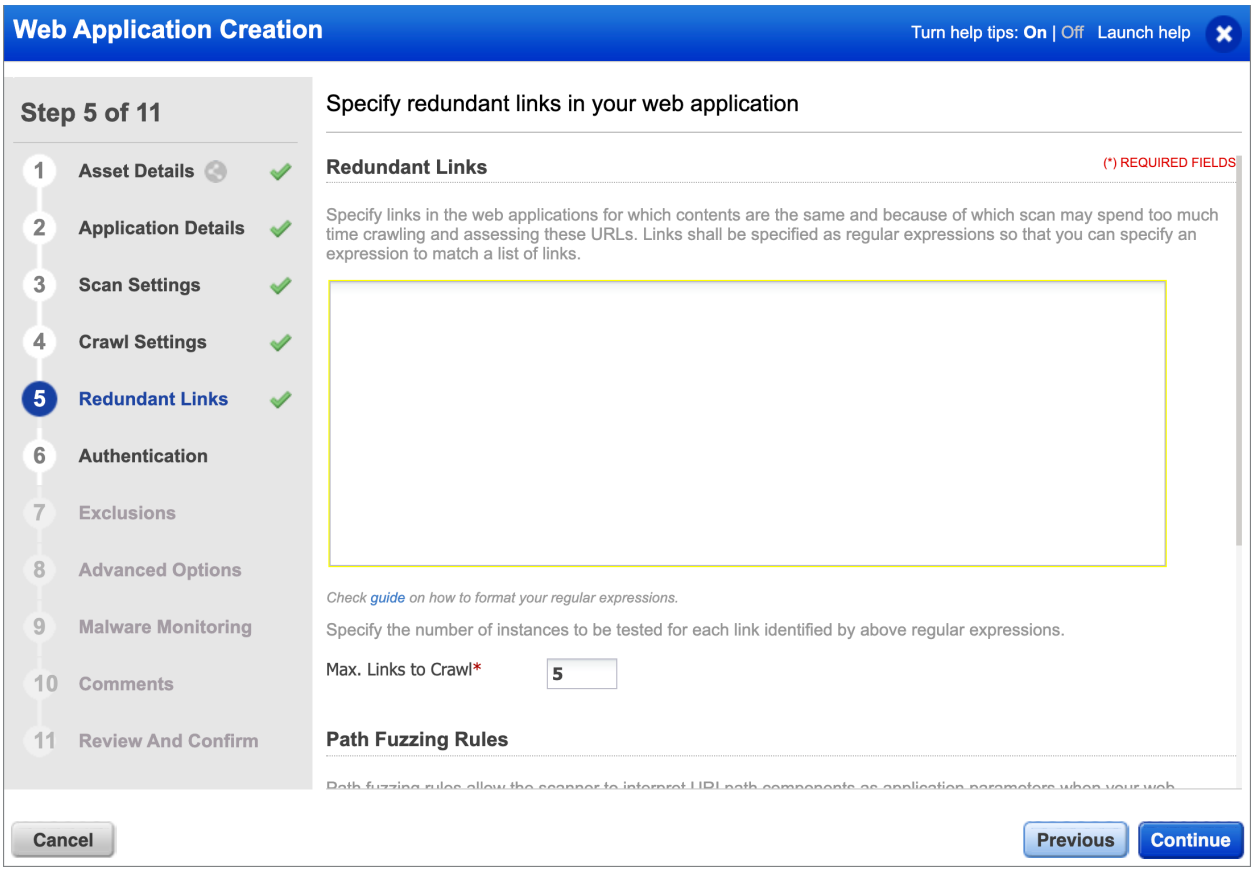
Crawling hints - Instruct the scan to adhere to existing configurations when scanning the web application using a robots.txt or sitemap.xml file

Header injection - Headers that need to be injected by our scanning service to scan the web application. This option is intended to be used when a workaround is needed for complex authentication schemes or to impersonate a web browser
Examples of header injection - https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/web_applications/scan_settings.htm



On Step 4 (Crawl Settings) of defining the web application, the following can be defined:

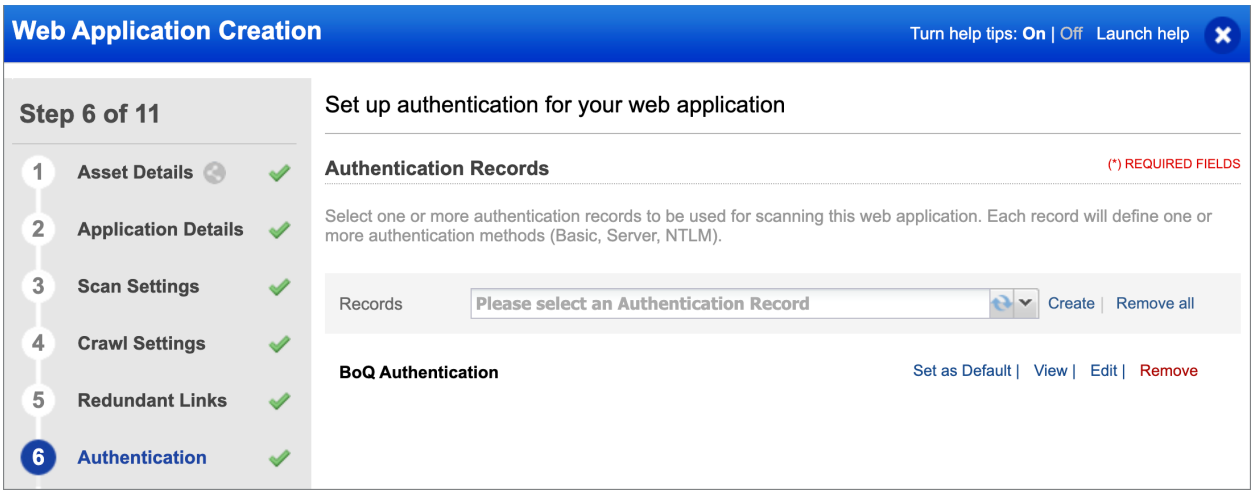
Selenium Script – Upload Selenium scripts recorded using Qualys Browser Recorder to play back functions in web applications during scanning



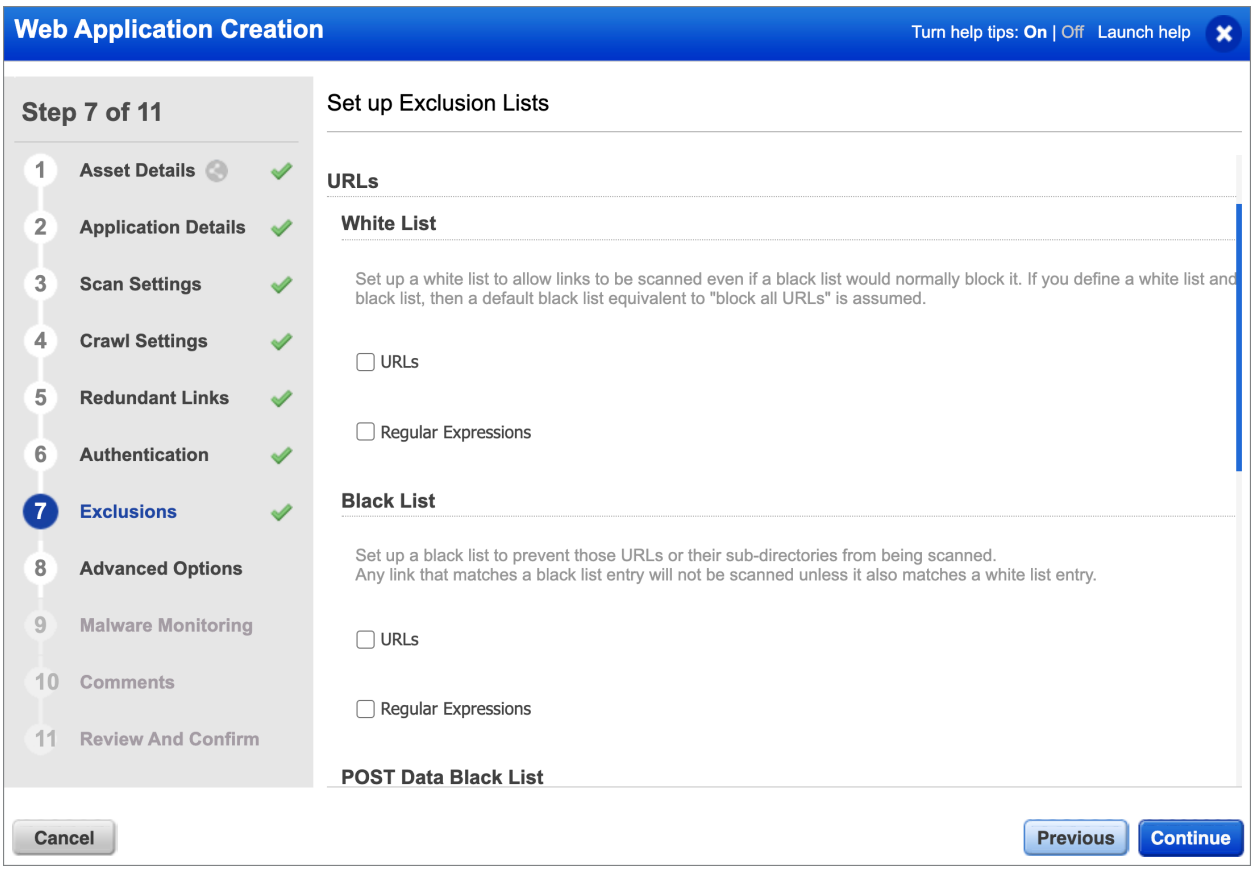
On Step 5 (Redundant Links) of defining the web application, the following can be defined:

Redundant Links – Links in the application that have the same content and may result in the scanner spending too much time crawling and assessing these URLs

Path Fuzzing Rules – If your application uses URL rewrite, use path fuzzing rules to specify the path components that need to be tested. More information can be found here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/path_fuzzing_rules.htm



On Step 6 (Authentication), you may define an authentication record to be used for authenticating into the web application.



On Step 7 (Exclusions) of defining the web application, the following can be defined:

White List – add URLs to white list to allow them to be scanned even if a black list would block it

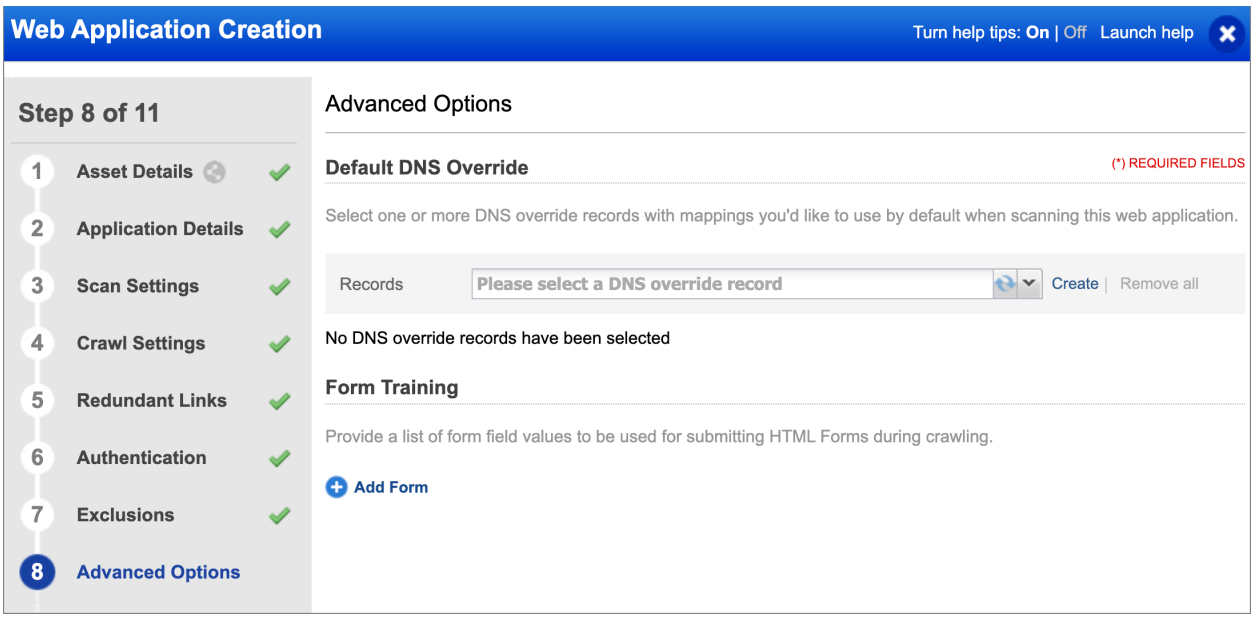
Black List – Add URLs to blacklist to prevent them and their sub-directories from being scanned

POST Data Black List - Define POST data lists to ensure blocking of form submission for POST requests in your web application as this could have unwanted side effects like mass emailing

Logout Regular Expression - Define logout regular expression to ensure that the logout links of your web application will not be scanned

Parameters – Define parameters to ensure these will be excluded from testing to improve scan efficiency

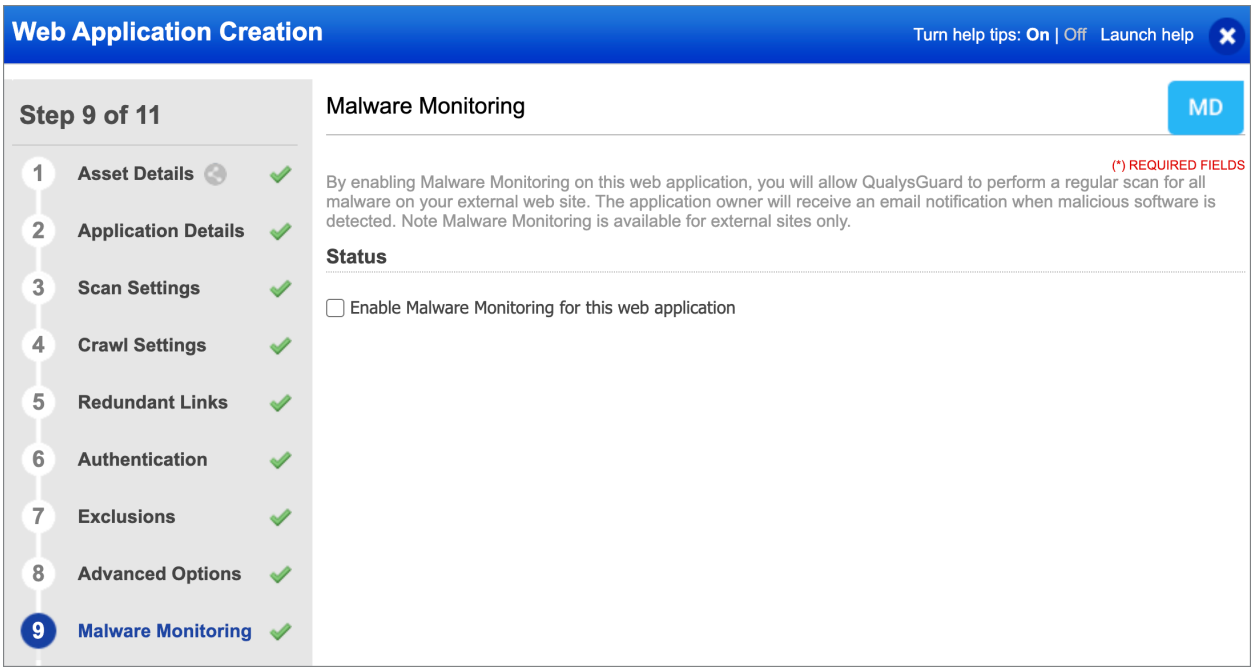
Read more about exclusion lists here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/web_crawling_and_black_lists.htm



On Step 8 (Advanced Options) of defining the web application, the following can be defined:

DNS Override - By default the scanner uses the DNS for the web application URL to crawl the web app and perform scanning. Select a DNS override record, to use the mappings in your record

Form Training - Define an action URI, specific form field and its value to be substituted during crawling and fuzzing. This feature allows you to override a specific field's value in any given form

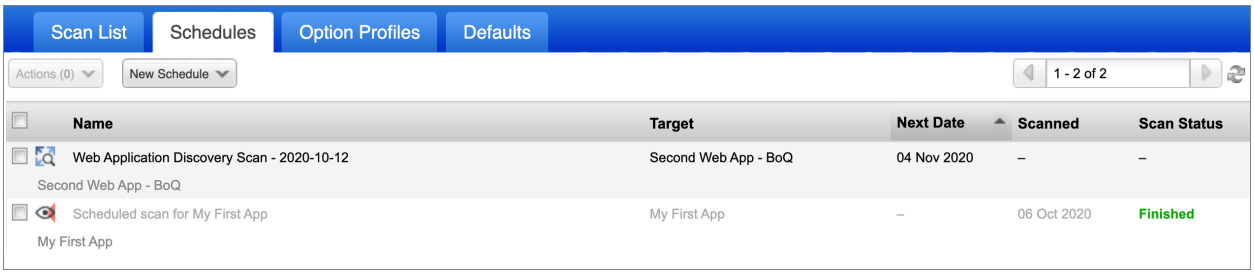


On Step 9 (Malware Monitoring), configure a malware scan to scan your web application for malwares. Read more here - https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/malware_monitoring.htm

Scheduled Scans

PLAY http://ior.ad/7f1T

Any scan that can be performed manually, can also be scheduled to run automatically, on a regular basis. This way you always have the most up-to-date security information in your account.

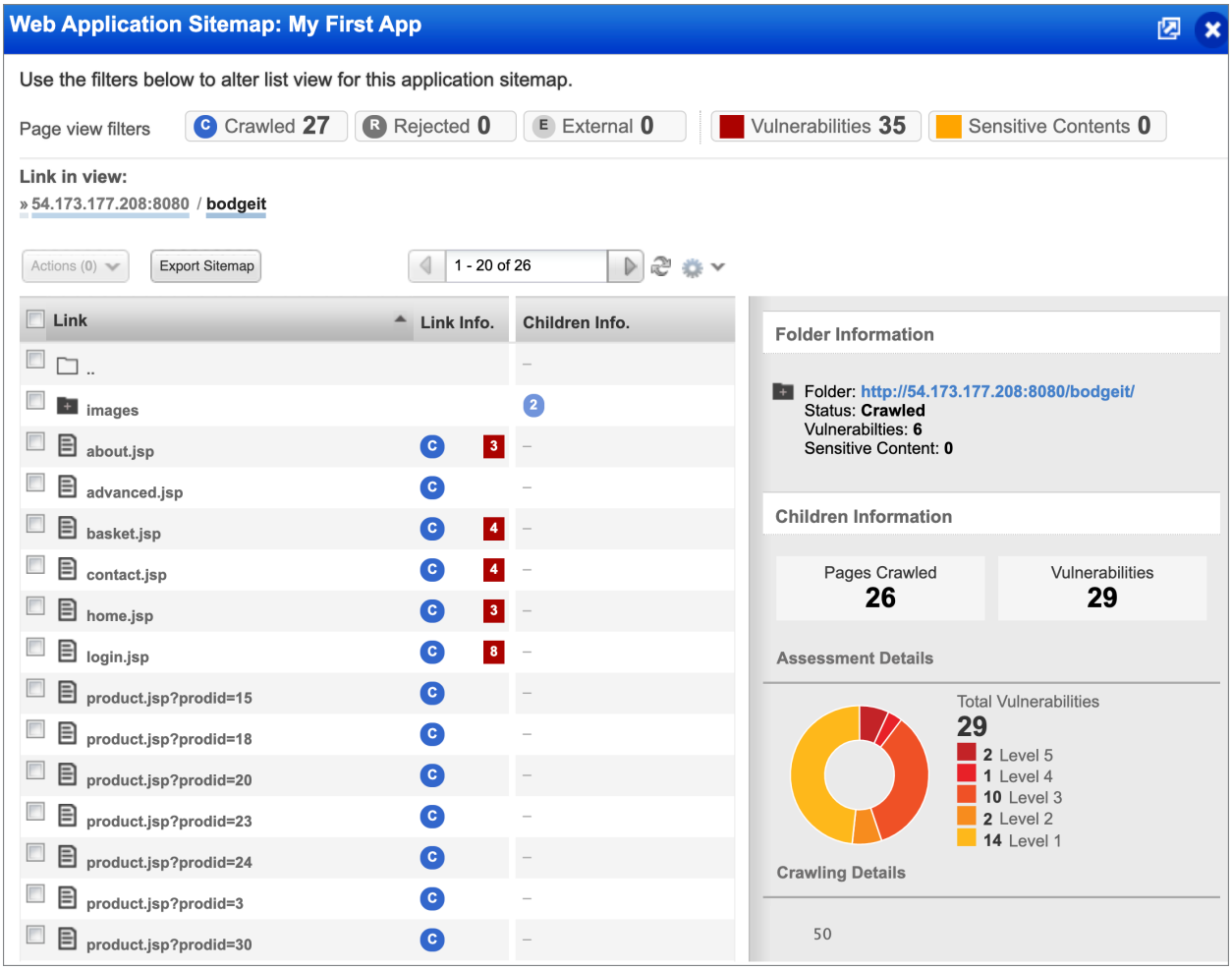


Setting up a scheduled scan is similar to setting up a regular WAS scan – provide information such as application and scanner appliance details, and then provide scheduling and notification information.

WAS Sitemap

PLAY http://ior.ad/7f2e

The Web Application Sitemap gives you a convenient way to get a list of all pages/links scanned with views on the links crawled, vulnerabilities and sensitive content detected.

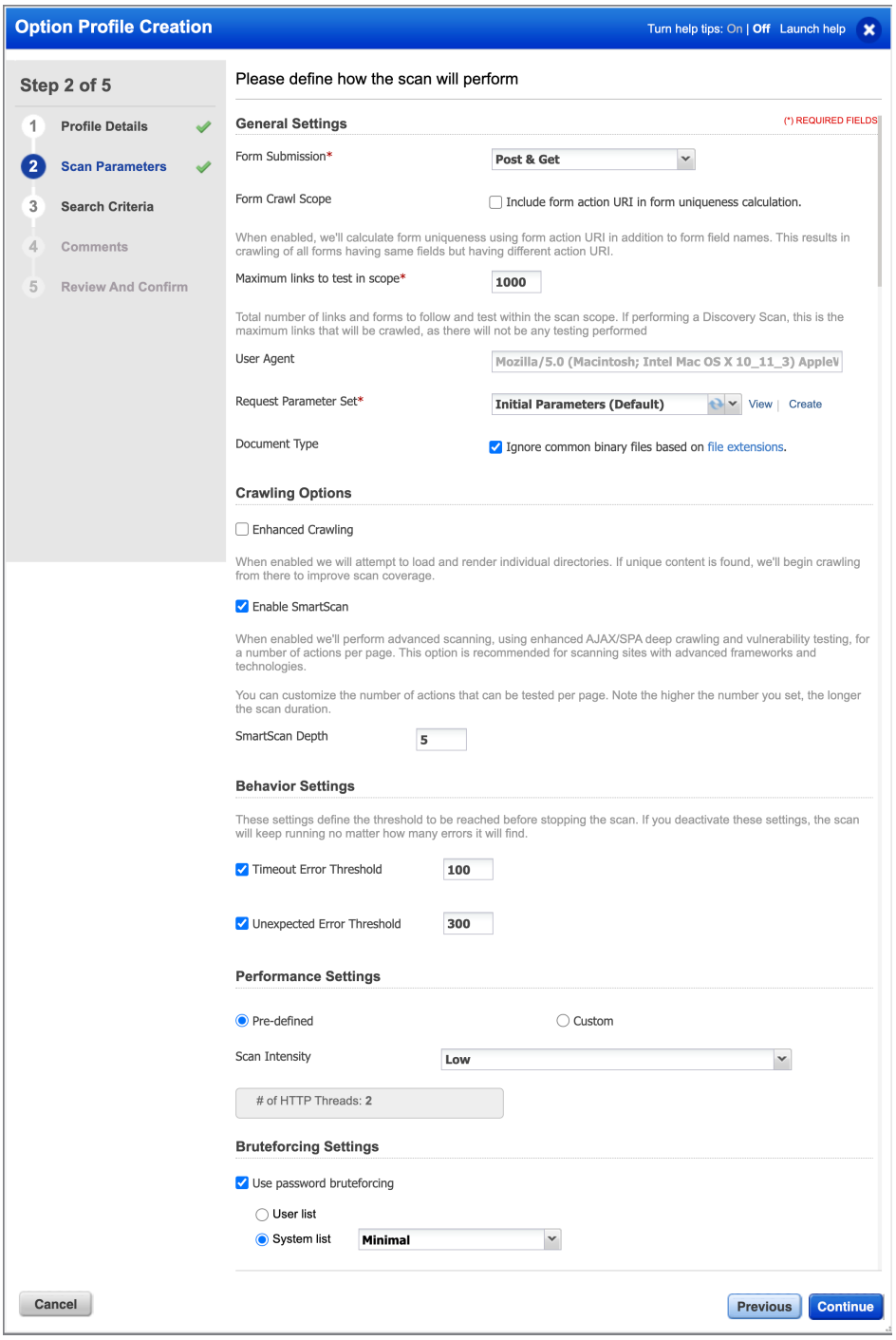


The following page view filters are available when viewing the sitemap:
Crawled – Only show pages that have been crawled during the scan
Rejected – Only show pages that have been rejected (this could be due scan permissions or configured blacklists)
External – Only show pages that contain external links (not in scope)
Vulnerabilities – Only show pages on which vulnerabilities have been detected
Sensitive content – Only show pages on which sensitive content has been detected (for example credit card numbers and social security numbers)

Option Profile

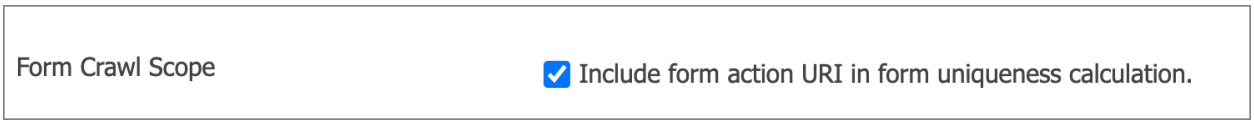
PLAY http://ior.ad/7f2o

The following options are available under the **Scan Parameters** section of an Option Profile:



Form Submission - When forms are submitted, http(s) uses GET or POST methods. The crawl can be limited to either type of form submission, both, and none. It is considered best practice to select "Post & Get" for the most thorough vulnerability analysis. If "none" is chosen, the only forms WAS will submit will be for authentication

Form Crawl Scope – By default, the scanner uses form names to determine the uniqueness of a form. When "Include form action URI in form uniqueness calculation" is enabled, the scanner uses the form action URI and the form field name to determine its uniqueness



Maximum links to test in scope – Specify the maximum links and forms to crawl during the scan. The maximum is 8000.

User Agent - If your web application requires specific user-agent string to access it, you need to specify the same. The default user agent setting that is used is user-agent: ***Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko) Version/9.0.3 Safari/601.4.4***

Request Parameter Set – Specify the default parameters that need to be injected into your web application, such as first name, last name, email address, phone number etc.

Document Type – Enable the "Ignore common binary files" option to not scan files with extensions pdf, zip, and doc.

Enhanced Crawling – When enabled, the scanner will attempt to load and render individual directories.

For example, if this link is found during crawling:
https://www.example.com/foo/abc/xyz/register.php

The scanner will make the first request to https://www.example.com/foo/abc/xyz and will then remove the directory "xyz" from the URL and crawl, https://www.example.com/foo/abc/ and later it will further remove "abc/" and will crawl https://www.example.com/foo/ .

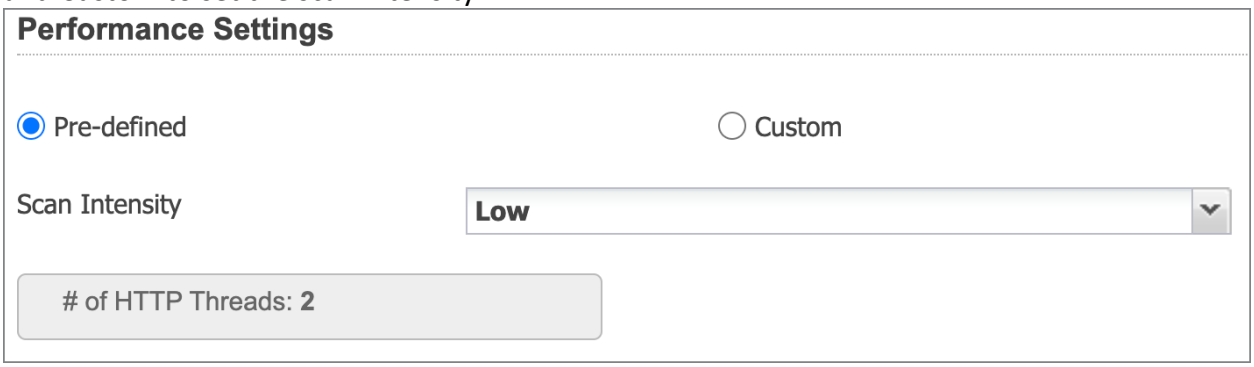
All links found during this process of removal and re-crawling will get added to the crawl queue, thus improving the scan coverage.

Enable SmartScan – When enabled, the scanner will perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing. This option is recommended for scanning applications with advanced frameworks and technologies.

Timeout Error Threshold – Maximum number of timeout errors encountered during the scan that will result in the scan being terminated.

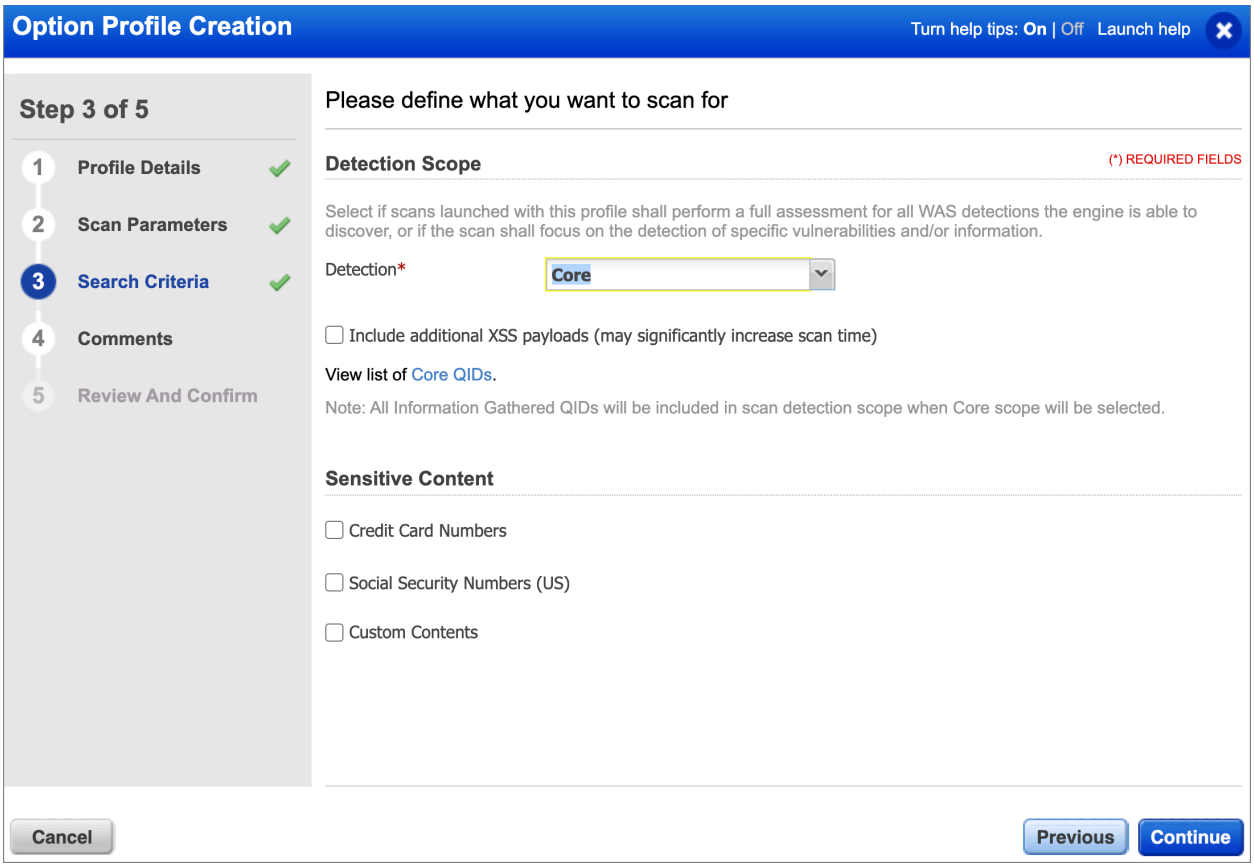
Unexpected Error Threshold - Maximum number of unexpected errors encountered during the scan that will result in the scan being terminated.

Performance Settings – select from Pre-defined (lowest, low, medium, high, and maximum) and Custom to set the scan intensity



Password bruteforcing – enable this to find out how vulnerable your web applications are to password-cracking techniques

The following options are available under the **Search Criteria** section of an Option Profile:



Detection Scope – This determines the vulnerabilities that will be checked during the scan:

- Core – Default for new WAS Option Profiles. Core scope includes vulnerabilities that Qualys considers most common in today's web applications. It does not include all the vulnerabilities that WAS can detect.
- Categories - Specific vulnerabilities defined in the categories. Select a category to check for associated vulnerabilities in the scan.
- Custom Search Lists - Specific vulnerabilities defined in Search Lists. This provides the most granular control over detection scope. You can select search lists to include and Search Lists to exclude.
- XSS Power Mode - Comprehensive tests for cross-site scripting vulnerabilities. The XSS Power Mode detection scope performs tests using the standard XSS payloads, which detect the most common instances of XSS, but also with additional payloads that can identify XSS in certain, less-common situations.
- Everything – All the vulnerabilities that WAS can detect.

Sensitive Content - Check for sensitive content in the web application pages it crawls based on known patterns (such as credit card numbers, social security numbers) or based on custom patterns you enter.

Qualys Browser Recorder Crawl Script

PLAY http://ior.ad/7f7S

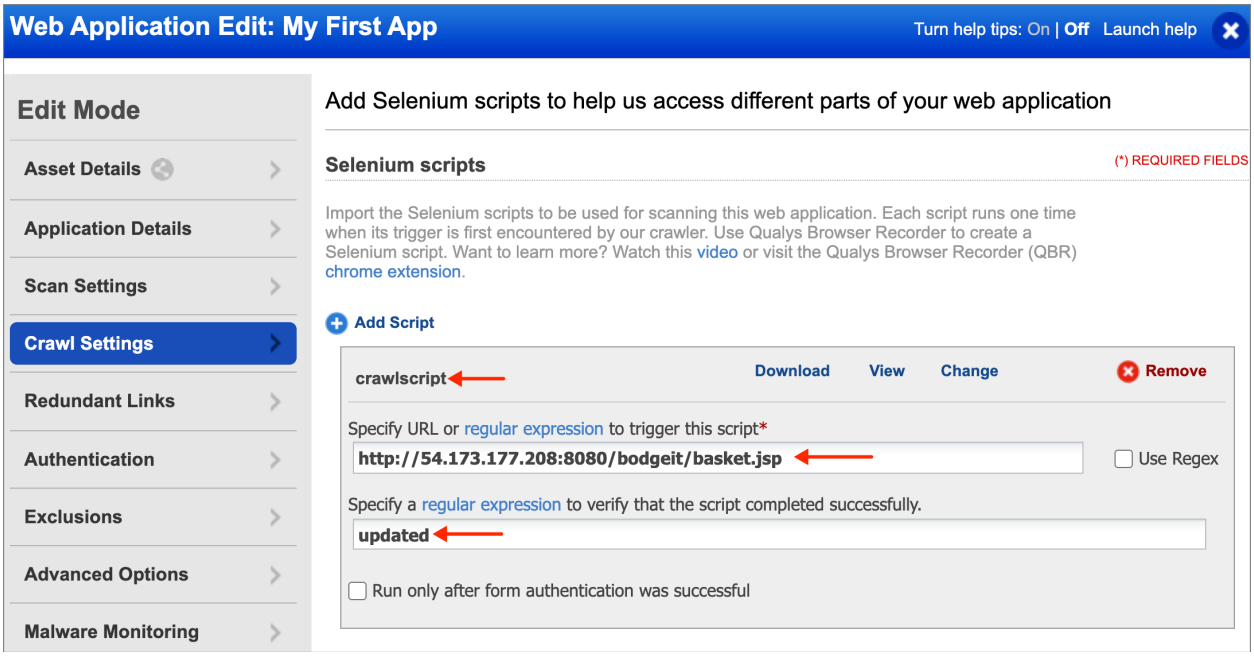
PLAY http://ior.ad/7f8a

Web applications often contain pages that require input from a knowledgeable application user, like the “Shopping Basket” page found in the BodgeIT Store.

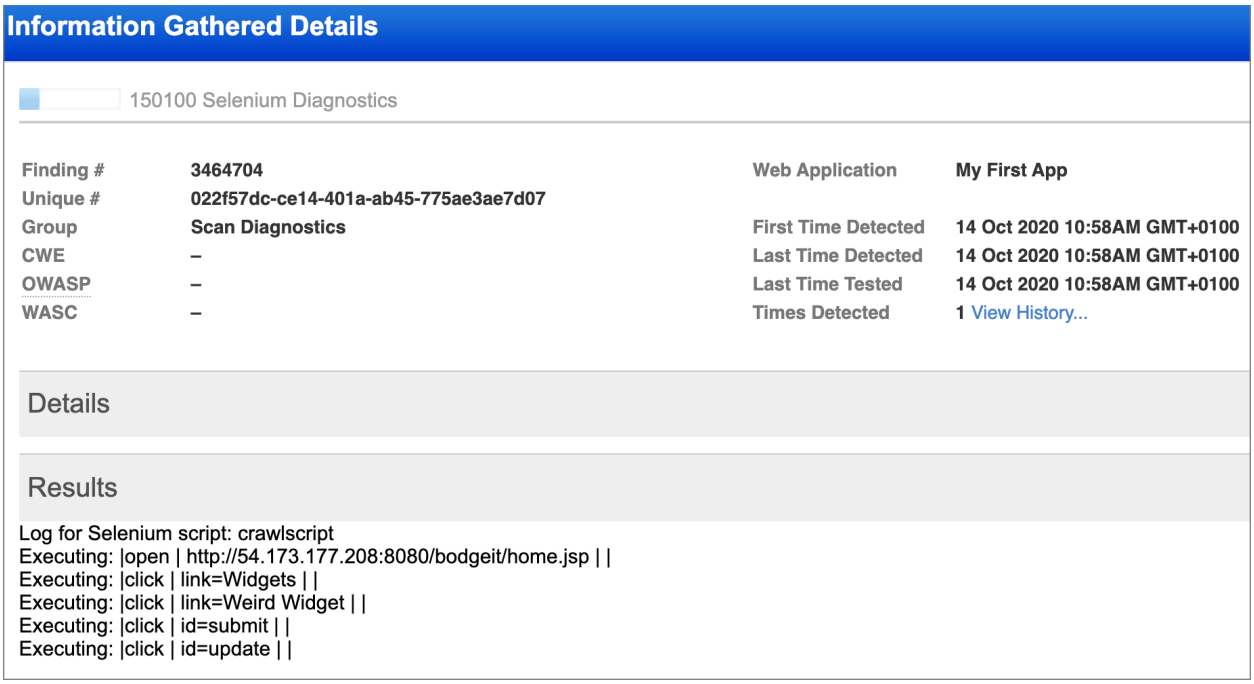
The QBR allows you to record your input decisions (e.g., keystrokes and mouse clicks) while you navigate the pages of any Web application. The script that is generated by QBR can then be replayed during your WAS scans, to perform your navigation steps and input decisions.

Detailed usage instructions for QBR can be found here - https://www.qualys.com/docs/qualys-browser-recorder-user-guide.pdf

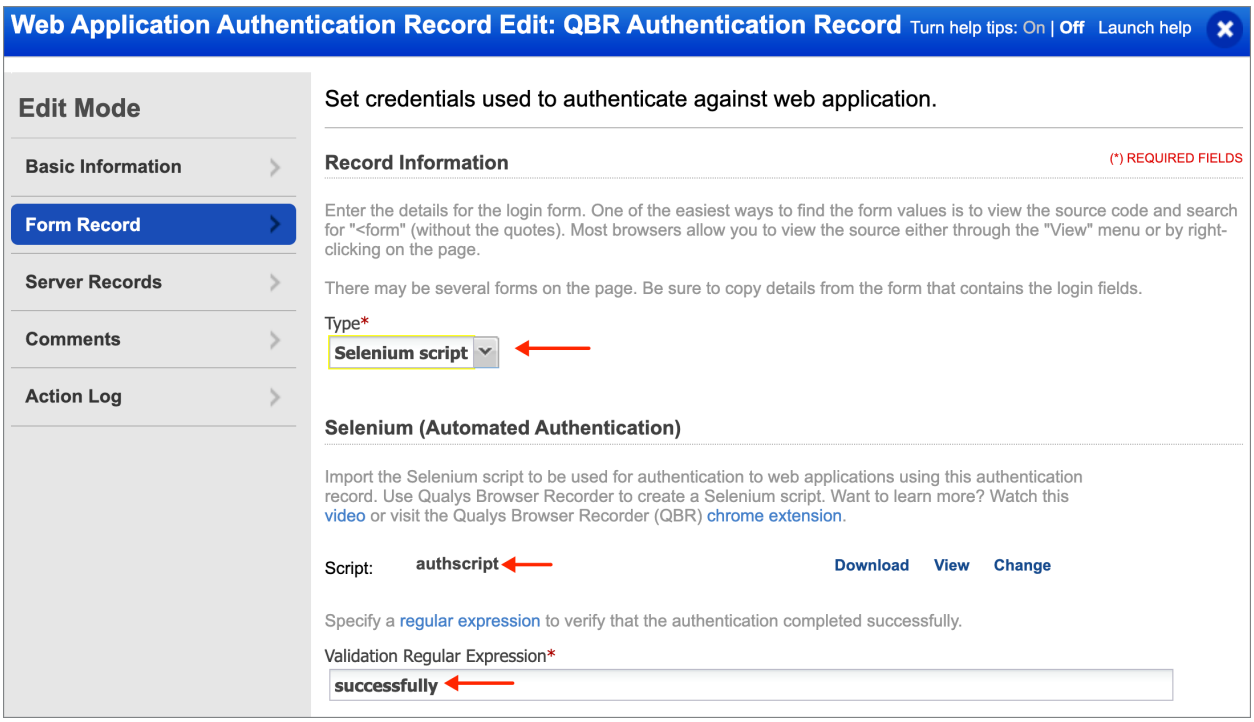
The crawl script can be uploaded to an application. This will cause the application to be crawled using the script.



When the scan is complete, look for QID 150100 to check for Selenium Diagnostics:



The authentication script can be used to create an authentication record.



WAS Reporting

PLAY http://ior.ad/7fmi

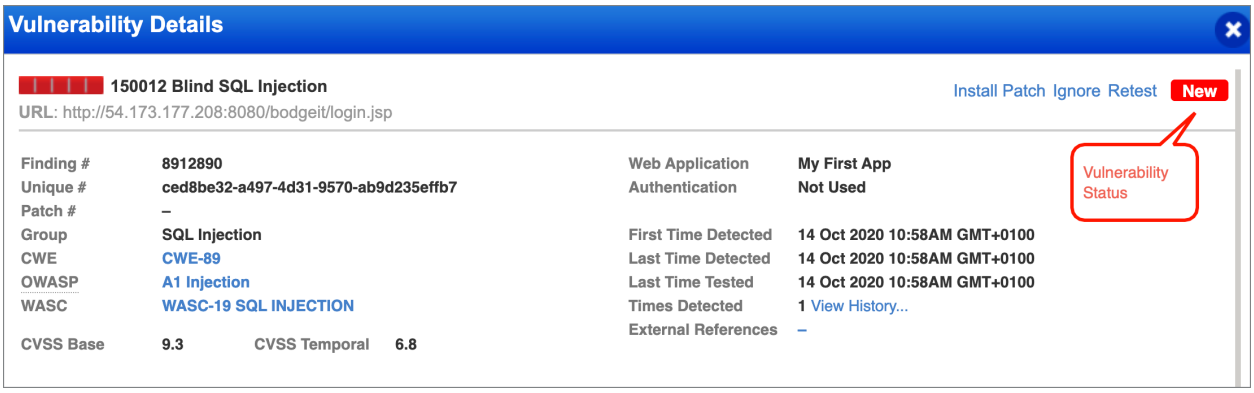
PLAY http://ior.ad/7ff3

Currently, the Qualys Web Application Scanning service offers 4 types of reports: Web Application Report, Scorecard Report, Scan Report, and a Catalog Report.

Web Application Report – Reports on aggregated findings from all scans.
Scan Report – Reports on findings from specific scans.
Scorecard Report – Provides an overall scorecard with high-level numbers and graphs.
Catalog Report – Provides a catalog of web services processed from completed maps, vulnerability scans and WAS scans.

Vulnerability status – Web application reports show the status of vulnerabilities, it may be one of the following:

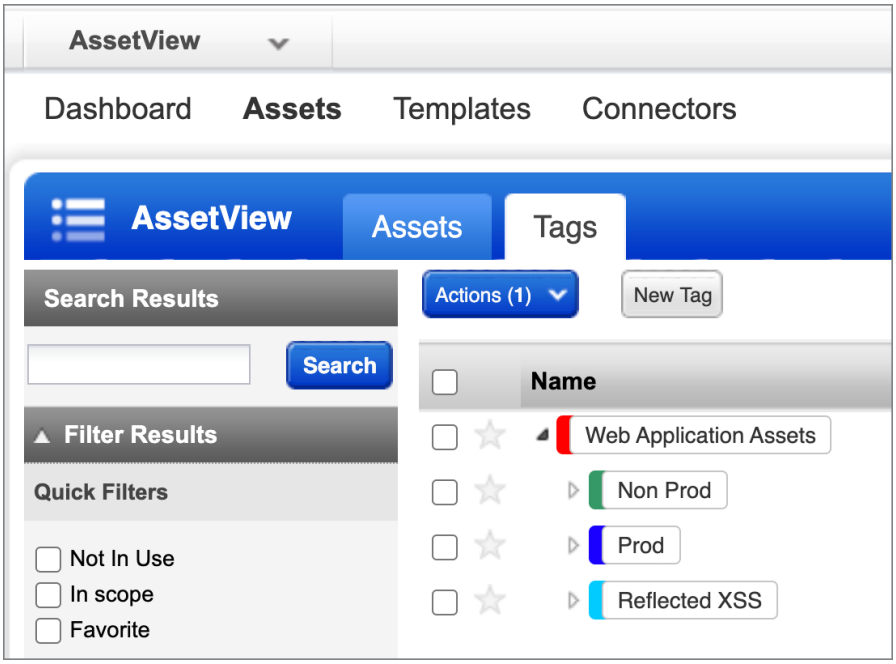
- New – vulnerabilities discovered for the first time in the latest scan
- Active – open vulnerabilities that have discovered more than once
- Fixed – vulnerabilities that have not been found in the latest scan
- Re-opened – vulnerabilities marked as fixed but detected again on the latest scan
- Ignored – vulnerabilities marked as ignored



Tagging

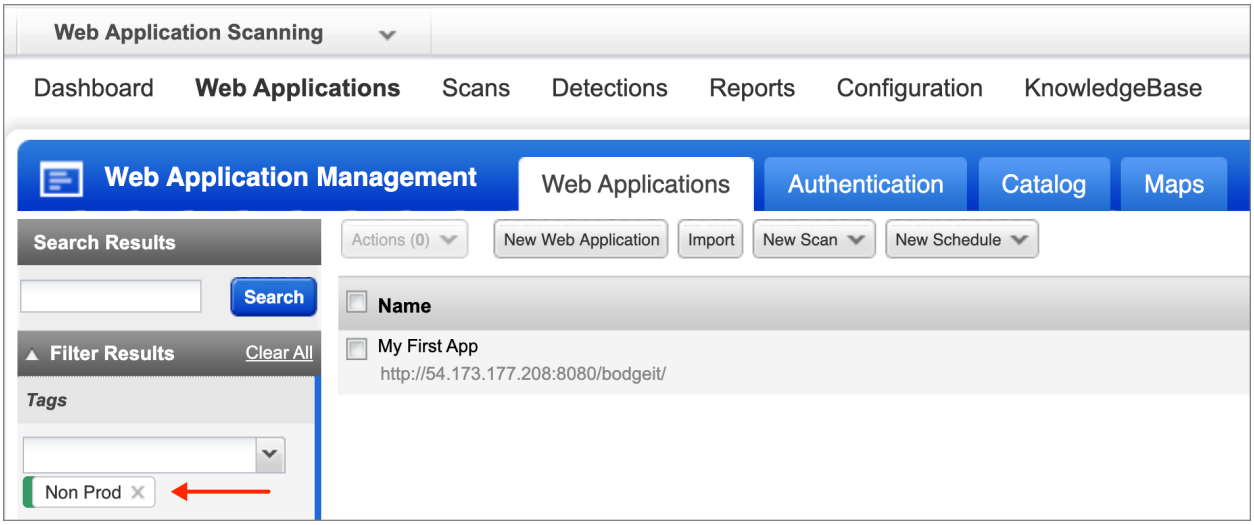
PLAY https://ior.ad/7T5W

Tags are labels that can be applied to web applications. Tags can be used for filtering, scanning, and reporting purposes.

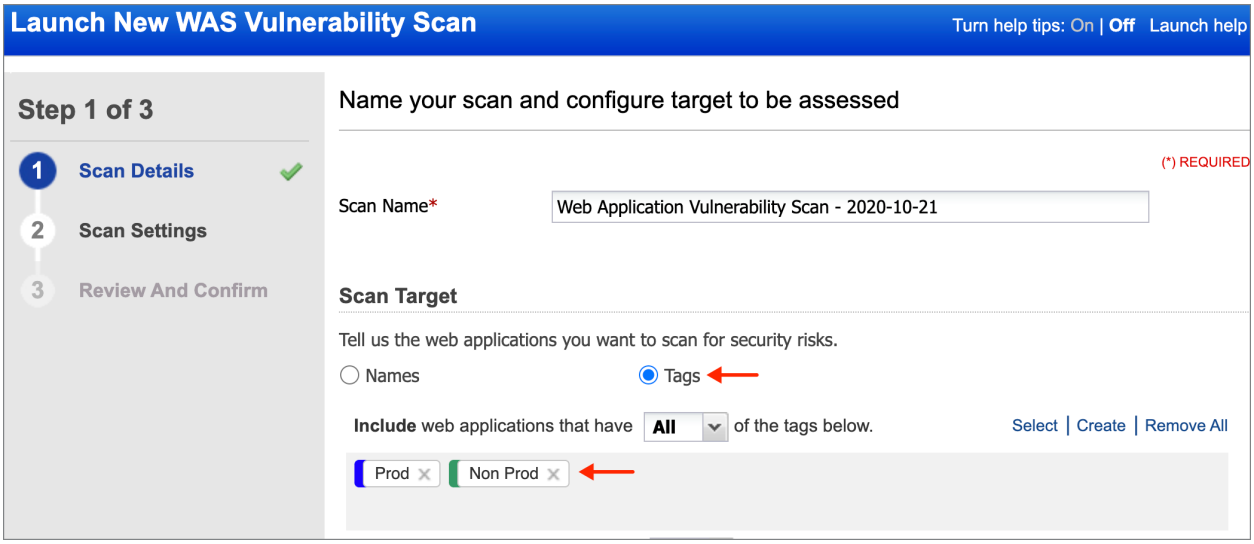


Tags are created from the AssetView application.

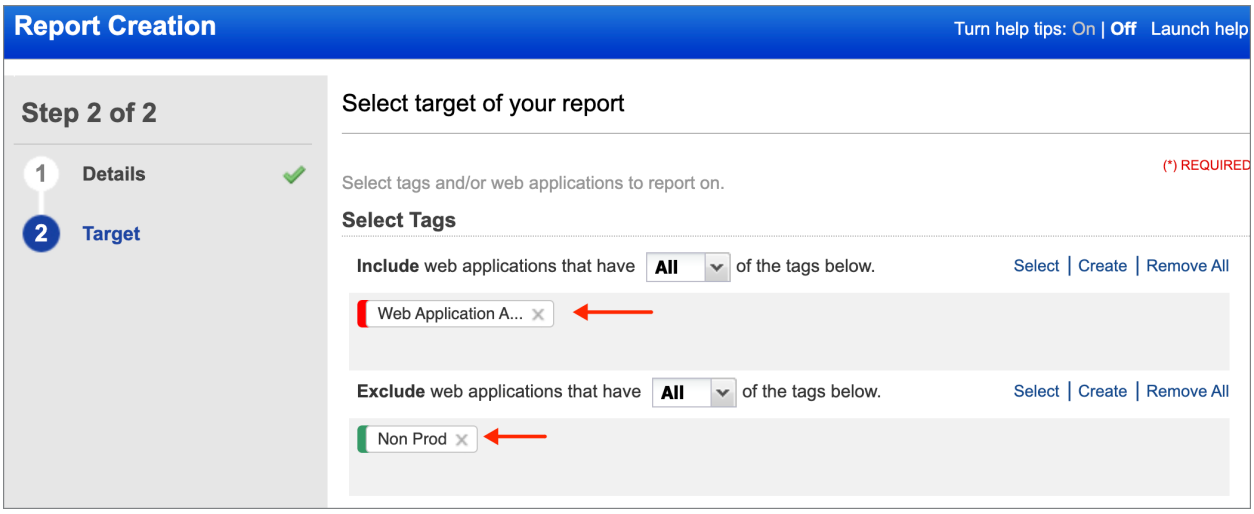
Use Tags for Filtering:



Use Tags for Scanning:



Use Tags for Reporting:



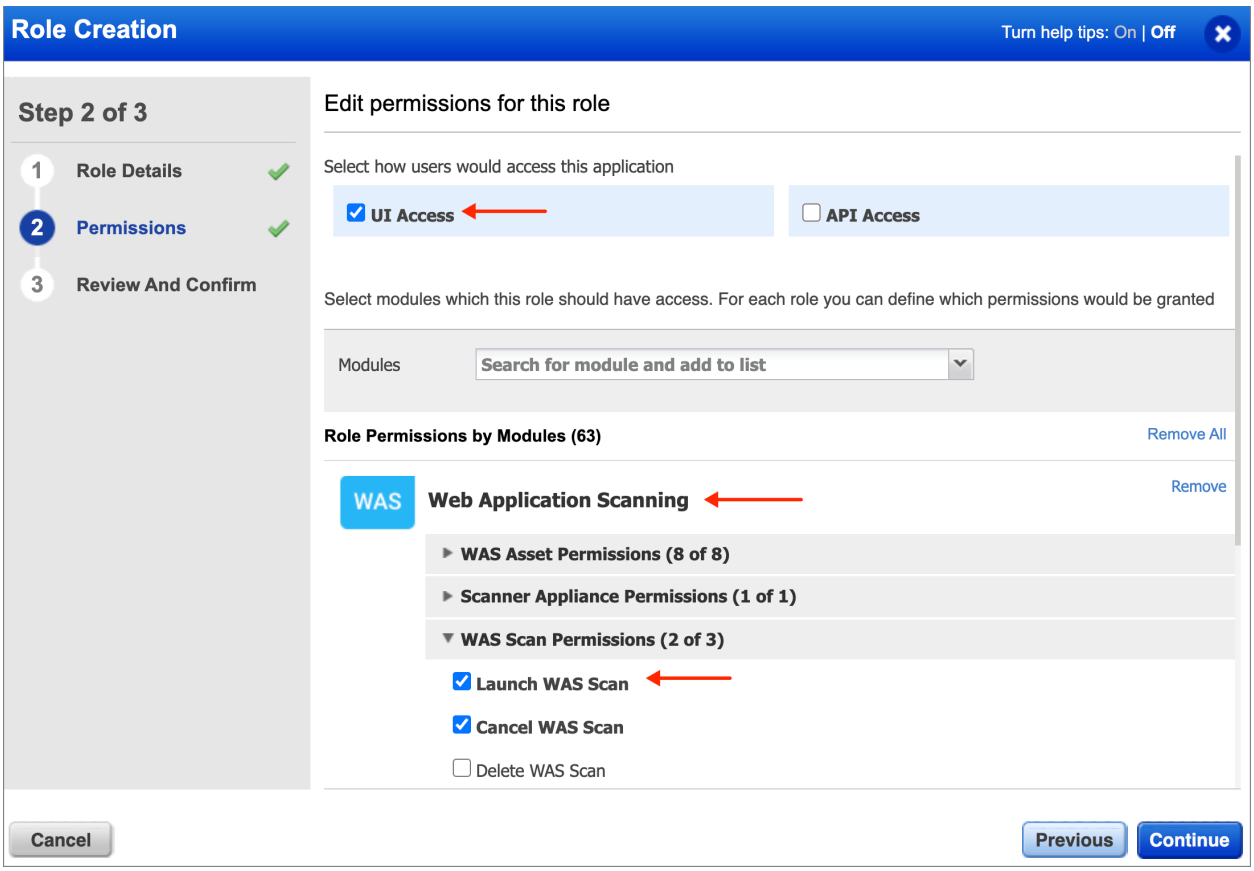
User Management

PLAY http://ior.ad/7fxv

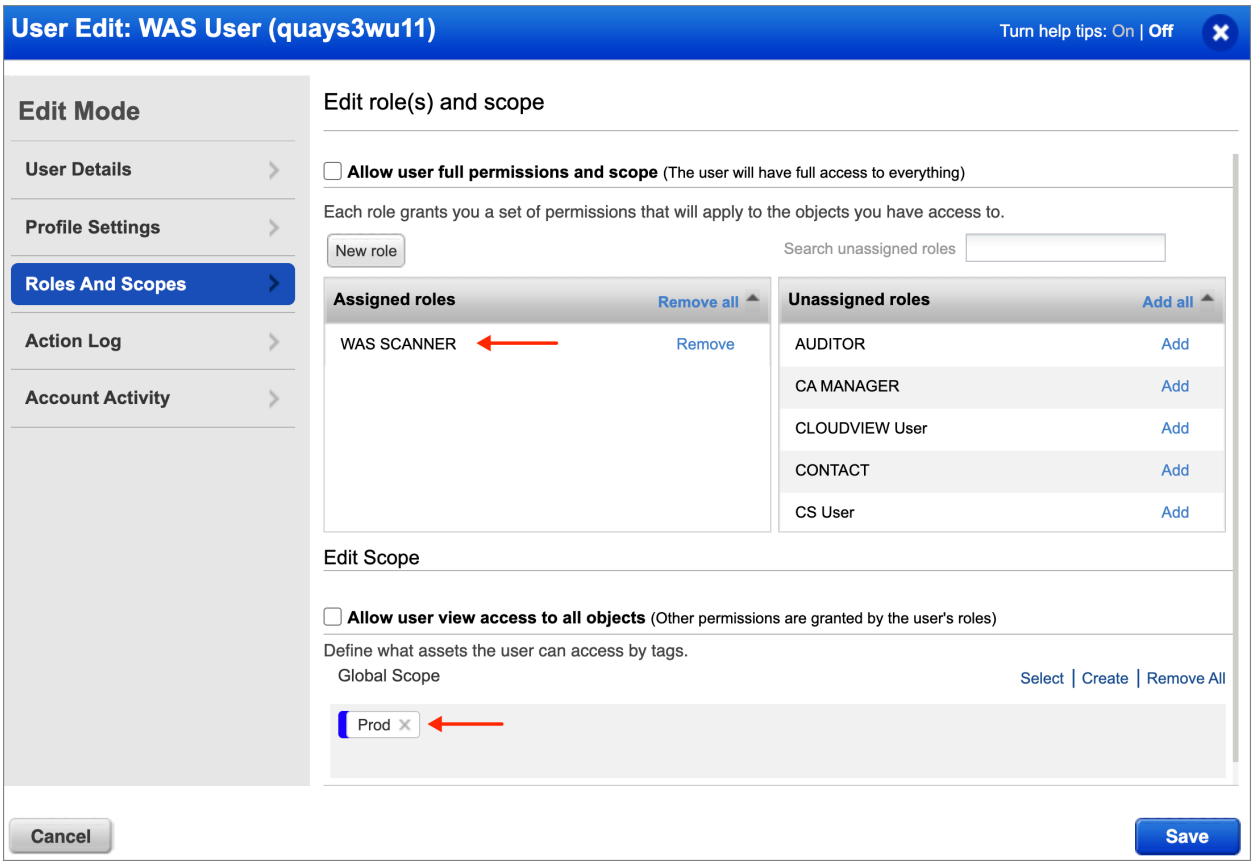
Users can be created from the Vulnerability Management (VM) or the Administration module. Once the user is created and activated, they will need to be given a scope and set of permissions from the interface.

Role Creation

To assign permissions to a user, first create a role from the Administration module. The role allows you to define the applications the user will have access to, how the user is allowed to access (UI or API), and permissions the user will have on the allowed applications.



By assigning the role to the user's profile, you can define the permissions available to the user. The scope of the user can be limited by attaching tags to the user's profile.

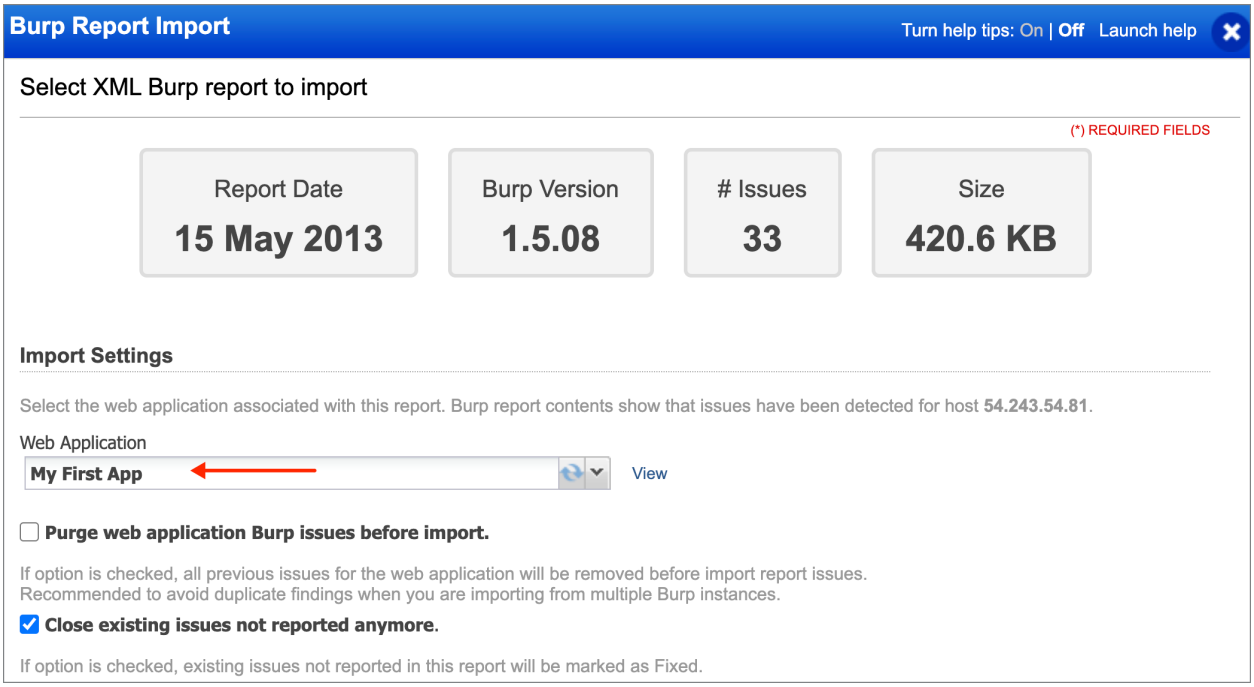

User Edit: WAS User (quays3wu11)
Turn help tips: On | Off
Edit Mode
User Details
Profile Settings
Roles And Scopes
Action Log
Account Activity
Edit role(s) and scope
Allow user full permissions and scope (The user will have full access to everything)
Each role grants you a set of permissions that will apply to the objects you have access to.
New role
Search unassigned roles
Assigned roles
Remove all
WAS SCANNER
Remove
Unassigned roles
Add all
AUDITOR
Add
CA MANAGER
Add
CLOUDVIEW User
Add
CONTACT
Add
CS User
Add
Edit Scope
Allow user view access to all objects (Other permissions are granted by the user's roles)
Define what assets the user can access by tags.
Global Scope
Select | Create | Remove All
Prod
Cancel
Save

Burp Integration

PLAY http://ior.ad/7fLy

Qualys offers integration with Burp. Burp is an attack proxy used for automated and manual penetration testing. This can be used in tandem with Qualys for sensitive applications that need thorough testing.

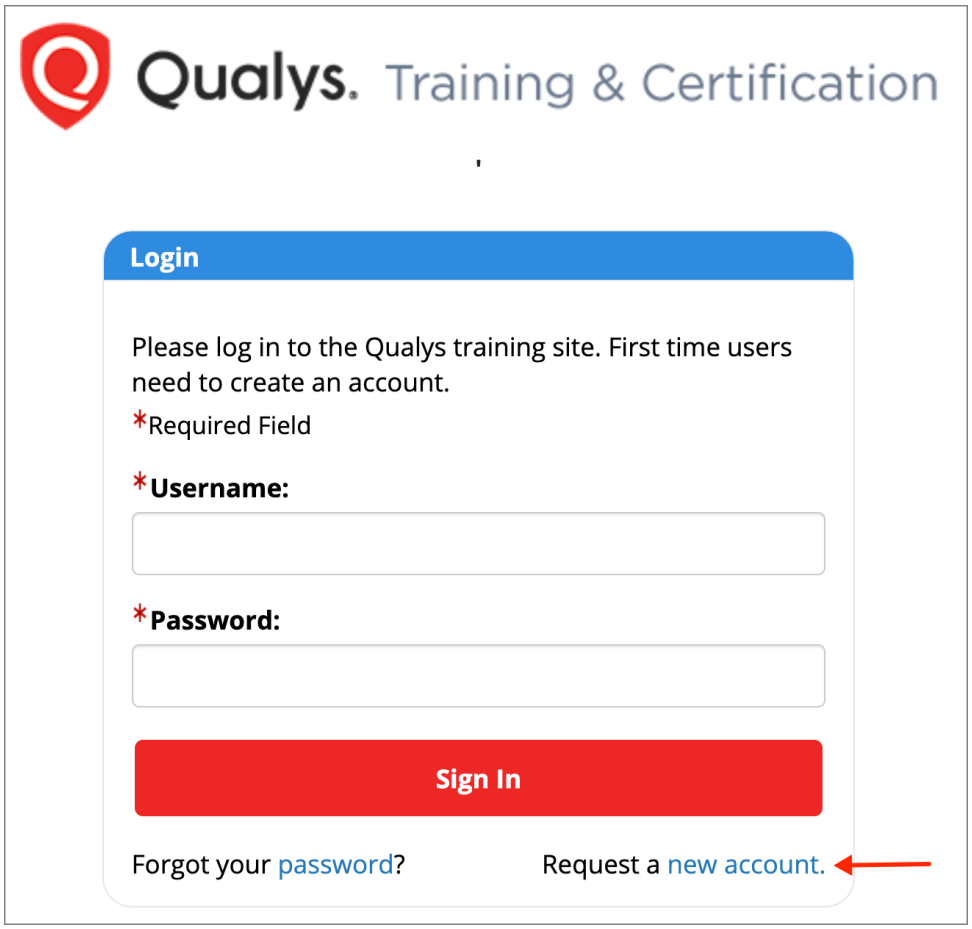
With this integration, Burp Suite Professional (BSP) results can be uploaded to Qualys. This allows Qualys to act as a centralized storage location for scan results from Burp, to go along with the results already obtained by the Qualys WAS service.



When importing BURP results into WAS, the BURP results must be associated with a specific Web Application.

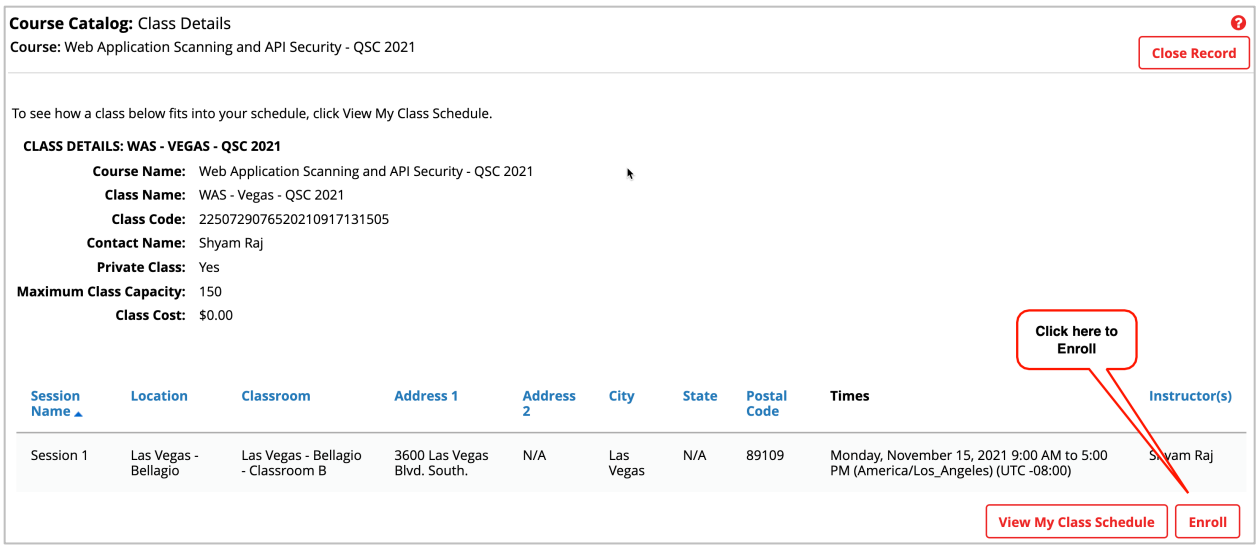
Qualys WAS Certification Exam

Participants in the Qualys Web Application Scanning and API Security training course have the option to take the Web Application Security Certification Exam. This exam is provided through our Learning Management System (LMS) at qualys.com/learning – candidates will need an account on this system to take the exam.



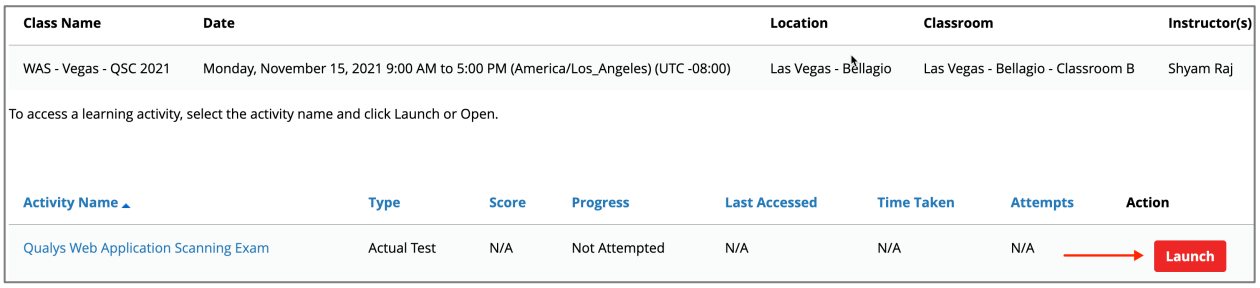
If you would like to take the exam, but do not already have a "learner" account, click the "Request a new account" link, from the LMS at http://qualys.com/learning.

Once you have created a "learner" account (and for those who already have an account), click the following link to access the "Qualys Web App and API Security – QSC 2021" course page: https://gm1.geolearning.com/geonext/qualys/scheduledclassdetails4enroll.geo?id=22511237829

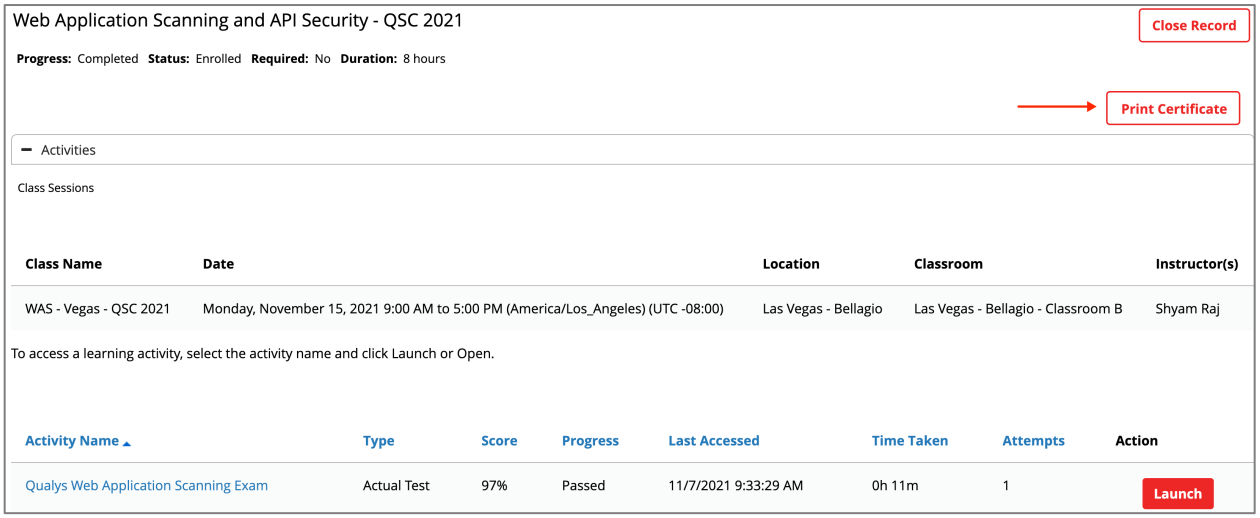


From the "Qualys Web App and API Security – QSC 2021" course page, click the "**Enroll**" button (lower-right corner).

After successfully completing the course enrollment, click the "Launch" button, for the Qualys Web Application Scanning Exam.



Each candidate is provided five attempts to pass the exam.



With a passing score of 75% (or greater), click the "Print Certificate" button to download and print your course exam certificate.

Training Survey

Please take a moment to take the survey about today's training - https://forms.office.com/r/rsy0Aja6Xz

Or scan the below link: